

# CYBER SLEUTH

## WHO CAUSED THE MISHAP?



### THE RECEPTIONIST

Frequently interacts with visitors and manages incoming communications, exposing her to spear-phishing emails and malicious attachments disguised as legitimate files.



### THE OFFICE MANAGER

Often handles sensitive company information like financial records and employee data, making him a prime target for phishing attacks and social engineering schemes.



### THE MARKETING DIRECTOR

Often uses third-party platforms to manage marketing campaigns and social media accounts, making him vulnerable to account hijacking.



### THE SALES REPRESENTATIVE

Constantly on the move, so often relies on mobile devices and public Wi-Fi, opening the possibility of cybercriminals intercepting and stealing sensitive data.

**INVESTIGATION FINDINGS:** It could have been anybody. Any employee, regardless of their role, is a target and can expose your business to cyberthreats.

A business has been the victim of a major data breach. Preliminary findings indicate it was an inside job, but we need your help to determine what happened.

**REACH OUT TODAY!**

LET'S BUILD A CYBER-SMART TEAM AND SHIELD YOUR BUSINESS FROM CYBERSECURITY MISHAPS.



TOUCAN  
TECHNOLOGY  
GROUP

(317) 376-4874

<https://toucan.tech>

FREE on-site  
consultations in  
greater  
Indianapolis!